

**IN THE UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF MISSOURI  
CENTRAL DIVISION**

MARCY A. JOHNSON,	)	
individually and on behalf of others	)	
similarly situated,	)	
	)	
Plaintiff,	)	Case No. 2:10-CV-04027-NKL
	)	
v.	)	
	)	
WEST PUBLISHING CORP.,	)	
	)	
Defendant.	)	

**ORDER**

This case concerns the sale by various states of their driver’s license databases to Defendant West Publishing Corp. (“West”), which then disseminates the personal information to third parties. The first question presented is whether the Driver’s Privacy Protection Act (“DPPA”) permits a reseller to obtain driver’s license information from a state when its sole purpose is to resell the information to third parties. The second question presented is whether a reseller can disclose the entire database to a business or individual having only a potential future use for some of the information sold, so long as there is no evidence of specific misuse, such as identity theft or stalking. The majority of courts which have decided these questions have concluded that the DPPA permits the practices. The Court disagrees.

**I. The Driver’s Privacy Protection Act**

In 1994, Congress enacted the DPPA to protect the privacy of drivers. The DPPA makes it generally “unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title.” 18 U.S.C. § 2722(a). Section 2721(b) is the first of two sections central to this case. It lists the fourteen permissible uses that are exceptions to the general rule prohibiting obtainment and disclosure of drivers’ personal information. Those uses are:

- (1) For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.
- (2) For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.
- (3) For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only-
  - (A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and
  - (B) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.
- (4) For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.

- (5) For use in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.
- (6) For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.
- (7) For use in providing notice to the owners of towed or impounded vehicles.
- (8) For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection.
- (9) For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49.
- (10) For use in connection with the operation of private toll transportation facilities.
- (11) For any other use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains.
- (12) For bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains.
- (13) For use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.
- (14) For any other use specifically authorized under the law of the State that holds the record, if such use is related to the operation of a motor vehicle or public safety.

18 U.S.C. § 2721(b).<sup>1</sup>

---

<sup>1</sup> Section 2721(a)(2) creates an even higher level of protection for “highly restricted personal information” – defined as “an individual’s photograph or image, social security number, medical or disability information” – which may be obtained or disclosed only with the consent of the individual or pursuant to the limited “uses permitted in subsections (b)(1), (b)(4), (b)(6), and (b)(9).” 18 U.S.C. §§ 2721(a)(2), 2725(4).

The second section in dispute provides that an “authorized recipient” may resell driver’s license information under certain limited circumstances:

(c) Resale or redisclosure. – An authorized recipient of personal information (except a recipient under subsection (b)(11) or (12)) may resell or redisclose the information only for a use permitted under subsection (b) (but not for uses under subsection (b)(11) or (12)). An authorized recipient under subsection (b)(11) may resell or redisclose personal information for any purpose. An authorized recipient under (b)(12) may resell or redisclose personal information pursuant to subsection (b)(12). Any authorized recipient (except a recipient under (b)(11)) that resells or rediscloses personal information covered by this chapter must keep for a period of 5 years records identifying each person or entity that receives information and the permitted purpose for which the information will be used and must make such records available to the motor vehicle department upon request.

18 U.S.C. § 2721(c).

The majority of courts reading these sections have concluded that they permit wholesale resellers to obtain in bulk every driver’s personal information so long as there is no evidence of specific misuse. *See, e.g., Taylor v. Acxiom Corp.*, 612 F.3d 325 (5th Cir. 2010). In other words, a reseller is not limited to obtaining personal information only for a specific customer qualified to use it by the DPPA, nor need the reseller itself have a right to the information under one of the fourteen exceptions to the DPPA’s rule of nondisclosure. In addition, the information can be sold in bulk to purchasers, even though the purchaser is only authorized under the DPPA to receive one piece of information. For example, according to the reasoning of *Taylor* and the majority of courts, since the DPPA permits driver’s license information to be disclosed “for use in providing notice to the owners of towed or impounded vehicles,” 18 U.S.C. § 2721 (b)(7),

a Cabool, Missouri tow truck operator may obtain the entire license database, including highly restricted personal information such as social security numbers, because one day the tow truck operator might need a single piece of information from the database. The majority of courts reason that so long as the private information is not actually used in a “prohibited” manner there is no violation of the DPPA. Yet the DPPA never explicitly lists any prohibited uses; rather, it generally prohibits all but the fourteen permissible uses enumerated in section 2721(b).

Having reviewed the language of the DPPA and its legislative history, the Court concludes that Congress did not intend the DPPA to authorize this widespread dissemination of private information untethered from the very uses that Congress listed in the DPPA.

## **II. Background**

On February 19, 2010, Plaintiff Marcy Johnson filed her Complaint [Doc. # 1], which made the following allegations. Defendant West is a corporation specializing in legal publishing, online information delivery, and various other legal information products. West has obtained, and continues to obtain, large databases of motor vehicle records containing personal information from each of the following states: Alabama, Alaska, Colorado, Connecticut, Florida, Idaho, Illinois, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Mexico, New York, North Dakota, Ohio, Tennessee, Texas, Utah, Wisconsin, Wyoming, and the District of Columbia (the “States”).

The information databases obtained by Defendant West from the States contained “personal information” and “highly restricted personal information” – as defined by the Driver’s Privacy Protection Act (“DPPA”), 18 U.S.C. §§ 2721, et seq. – belonging to millions of licensed drivers, including Johnson and the putative class members.

Defendant made the information available for search and sale on the Internet via websites that it controlled and operated. The personal information or highly restricted personal information of Plaintiff and the putative class members was obtained and disseminated by Defendant for purposes not permitted under the DPPA. Plaintiff has suffered damages as a result of Defendant’s conduct.

Plaintiff Johnson’s Complaint proposes the following class definition:

All individuals with a motor vehicle registration on file in the States of Alabama, Alaska, Colorado, Connecticut, Florida, Idaho, Illinois, Iowa, Kentucky, Louisiana, Main[e], Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Mexico, New York, North Dakota, Ohio, Tennessee, Texas, Utah, Wisconsin, Wyoming and the District of Columbia, whose personal information or highly restricted personal information, as defined by 18 U.S.C. §§ 2725(3) and (4), was obtained, disclosed, or sold by Defendant, or any agent, officer, employee, or contractor of Defendant (the “Class”). The Class excludes Defendant’s directors, officers, parent corporations, subsidiaries, and affiliates.

[Doc. # 1 at ¶ 15.]

The Complaint sets forth three Counts. Count I asserts a violation of the DPPA: “Defendant knowingly obtained, disclosed, and/or sold Plaintiff’s and the putative Class members’ personal information or highly restricted personal information, as defined by the DPPA, for a use or uses not permitted under the statute.” *Id.* at ¶ 29. Count I prays

for damages. Count II asserts a claim for unjust enrichment and seeks disgorgement. Finally, Count III asserts a claim for injunctive relief, based on DPPA violations.

On May 11, 2010, the Court granted Defendant West's Motion to Dismiss Count II of Plaintiff's Complaint. [Doc. # 22.] West's motion had been based primarily on this Court's reasoning in another DPPA case, *Wiles v. Southwestern Bell Tel. Co.*, No. 09-4236-CV-C-NKL (W.D. Mo. Apr. 13, 2010). [Doc. # 19, Ex. 1.]

Defendant West now moves for a judgment on the pleadings.

### **III. Judgment on the Pleadings Standard**

When considering a motion for a judgment on the pleadings, the Court accepts as true all facts pleaded by the nonmoving party and grants all reasonable inferences from the pleadings in favor of the nonmovant. *Poehl v. Countrywide Home Loans, Inc.*, 528 F.3d 1093, 1096 (8th Cir. 2008) (citing *Syverson v. FirePond, Inc.*, 383 F.3d 745, 749 (8th Cir. 2004)). A judgment on the pleadings is appropriate "where no material issue of fact remains to be resolved and the movant is entitled to judgment as a matter of law." *Id.* (quoting *Faibisch v. Univ. of Minn.*, 304 F.3d 797, 803 (8th Cir. 2002)). The standard of review for a Rule 12(c) motion is essentially the same as for Rule 12(b)(6). *See Westcott v. City of Omaha*, 901 F.2d 1486, 1488 (8th Cir. 1990); *Clemons v. Crawford*, 585 F.3d 1119, 1124 (8th Cir. 2009). A complaint must plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "[O]nce a claim has been stated adequately, it may be supported by showing any set of facts consistent with the allegations in the complaint." *Id.* at 563 (citation omitted).

#### IV. Statutory Construction Standard

Plaintiff Johnson argues that the DPPA must be liberally construed consistent with its overriding purpose to protect drivers' privacy. Even though some courts have referred to the DPPA as remedial, "[t]he mere fact that a statute is characterized as 'remedial' . . . is of little value in statutory construction unless the term 'remedial' has for this purpose a more discriminate meaning" than simply providing legal remedies. 3 Norman J. Singer & J.D. Shambie Singer, *Statutes and Statutory Construction* § 60:2, at 267 (7th ed. 2008) [hereinafter *Sutherland Statutory Construction*]. For purposes of statutory construction, "[u]sually 'remedial' is used in connection with legislation which is not penal or criminal in nature . . . ." *Id.* at 268. Within the DPPA, section 2723(a) provides for the possibility of a "Criminal fine." 18 U.S.C. § 2723(a).

On the other hand, the mere fact that one of the DPPA's possible enforcement mechanisms is a criminal fine does not trigger a lenient interpretation. Even for statutes that are entirely penal in nature:

In most respects, the interpretation of penal laws does not differ from the construction of other statutes. The standard of decision is either the intent of the legislature or what the statute means to others, and the determination of such relies on other canons of statutory construction. A court's primary objective is to ensure that the purpose of the legislature is accomplished.

*Sutherland Statutory Construction, supra*, § 59:8, at 226. As the Eighth Circuit has explained: "[T]he rule that a penal statute is to be strictly construed in favor of persons accused, is not violated by allowing the language of the statute to have its full meaning, where that construction supports the policy and purposes of the enactment." *Wilson v.*



*United States*, 77 F.2d 236 (8th Cir. 1935) (citations omitted); *see also United States v. R.L.C.*, 915 F.2d 320, 325 (8th Cir. 1990) (“The rule of lenity states that a court cannot interpret a federal criminal statute so as to increase the penalty that it places on an individual when such an interpretation can be based on no more than a guess as to what Congress intended.” (internal quotation and citation omitted)).

Because neither the remedial statute rule of liberal construction nor the criminal law rule of lenity apply to these circumstances, the Court declines to give either a liberal construction or a lenient construction to the statute. Instead, the Court interprets the DPPA in accordance with its plain language and legislative purpose. This “plain meaning” or “plain language” rule of statutory interpretation “requires examining the text of the statute as a whole by considering its context, ‘object, and policy.’” *Harmon Indus., Inc. v. Browner*, 191 F.3d 894, 899 (8th Cir. 1999) (quoting *Pelofsky v. Wallace*, 102 F.3d 350, 353 (8th Cir. 1996)). Resort to legislative history is appropriate when a statute is ambiguous or to show that the plain reading of the text would be “demonstrably at odds with the intentions of its drafters, and those intentions must be controlling.” *Owner-Operator Indep. Drivers Ass’n v. United Van Lines, LLC*, 556 F.3d 690, 695 (8th Cir. 2009) (quoting *Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 571 (1982)).

## **V. Plaintiff’s Claim and West’s Defenses**

Plaintiff Johnson brings this class action under section 2724(a) of the DPPA: “A person who knowingly obtains, discloses, or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the

individual to whom the information pertains, who may bring a civil action in a United States district court.” 18 U.S.C. § 2724(a). Defendant West argues that (1) “obtainment for the purpose of reselling information for permissible uses does not violate the Act” [Doc. # 31 at 11]; and (2) “[a]bsent an allegation of misuse by West or its customers,” the DPPA violation alleged in Plaintiff’s Complaint is implausible because bulk sale of personal information is permissible under the statute. [Doc. # 40 at 9.]

## **VI. Is the Mere Purpose of “Reselling Information for Permissible Uses”**

### **Sufficient to Authorize the Receipt of Personal Information under the DPPA?**

Defendant’s Motion for Judgment on the Pleadings is based primarily on West’s contention that this Court’s reasoning in *Roberts v. Source for Public Data*, 2008 WL 5234675 \*1 (W.D. Mo. Dec. 12, 2008), should be reevaluated in light of the Fifth Circuit’s decision in *Taylor v. Acxiom Corp.*, 612 F.3d 325 (5th Cir. 2010). According to West, in *Roberts*

this Court interpreted the DPPA as limiting those who may resell motor vehicle information to only those who first used the information themselves for one of the fourteen permitted uses. In other words, this Court construed the phrase “authorized recipient” to mean “authorized user.”

[Doc. # 31 at 2.]

The Court cannot accept the premise of Defendant’s motion. In *Roberts*, this Court did not intend to suggest that no personal information could be resold before it is used. As Plaintiff Johnson notes, *Roberts* concluded that “it is clear from the context in

section 2721(c) that an authorized recipient is one who has received the information pursuant to one of the 2721(b) exceptions.” *Roberts*, 2008 WL 5234675 at \*3.

On this Motion for Judgment on the Pleadings, Defendant West does not argue that it obtained states’ driver’s license database because it qualified under one of the fourteen exceptions to the DPPA’s default rule of nondisclosure. Instead, as a reseller, West relies on section 2721(c) for its authority to obtain states’ databases of personal information.

That section states:

(c) Resale or redisclosure. – An authorized recipient of personal information (except a recipient under subsection (b)(11) or (12)) may resell or redisclose the information only for a use permitted under subsection (b) (but not for uses under subsection (b)(11) or (12)). An authorized recipient under subsection (b)(11) may resell or redisclose personal information for any purpose. An authorized recipient under (b)(12) may resell or redisclose personal information pursuant to subsection (b)(12). Any authorized recipient (except a recipient under (b)(11)) that resells or rediscloses personal information covered by this chapter must keep for a period of 5 years records identifying each person or entity that receives information and the permitted purpose for which the information will be used and must make such records available to the motor vehicle department upon request.

18 U.S.C. § 2721(c).

#### **A. The Plain Meaning of the Text**

Based on the language of the DPPA, the Court concludes that Congress used the term “authorized recipient” in section 2721(c) to refer to those persons or entities that obtained the information pursuant to one or more of the fourteen exceptions immediately preceding the reference to “authorized recipient.” Rather than writing “an individual or entity obtaining personal information for uses authorized by the preceding section,”

Congress wrote “authorized recipient” – not a particularly surprising shorthand in the annals of statutory construction. This conclusion is grounded in the express language of the DPPA as well as its legislative history.

First, sections 2721(a) and 2722(a) make nondisclosure of personal information the default rule. *See* 18 U.S.C. § 2721(a) (“In general” prohibiting disclosure of personal information “except as provided in subsection (b)”); 18 U.S.C. § 2722(a) (“It shall be unlawful for any person knowingly to obtain or disclose personal information . . . for any use not permitted under section 2721(b) of this title.”). Section 2721(b) then lists fourteen discrete exceptions to nondisclosure. One would expect that if Congress had intended to make a fifteenth exception to the nondisclosure rule, it would have mentioned it while listing the exceptions to the rule of nondisclosure.

Second, the language of section 2721(c) supports the Court’s conclusion. According to that section, “[a]n authorized recipient of personal information (except a recipient under subsection (b)(11) or (12)) may resell or redisclose the information only for a use permitted under subsection (b) (but not for uses under subsection (b)(11) or (12)). An authorized recipient under (b)(11) may resell or redisclose personal information for any purpose. An authorized recipient under section (b)(12) may resell or redisclose personal information pursuant to subsection (b)(12).” 18 U.S.C. § 2721(c). In each sentence of section 2721(c) Congress linked the term “authorized recipient” to the specific section of 2721(b), that had authorized the release of the information to the recipient. The only explanation for this is that Congress intended authorized recipients to

be individuals or entities, or their agents, qualified to receive the information by the terms of section 2721(b). To read section 2721(c) otherwise would lead to the absurd result that resellers could obtain all of the personal information in the database simply by calling themselves resellers, while everyone else – including law enforcement – would have to justify their receipt of personal information under the 2721(b) exception applicable to them.

Similarly, as discussed further below, Defendant West’s interpretation produces the absurd result of resellers having far greater latitude to obtain and disclose information than do persons who obtain information under section 2721(b)(12) for bulk distribution of commercial surveys and solicitations. Section 2721(b)(12) is the only DPPA exception which makes reference to “bulk distribution,” and it requires that individuals opt in by providing their express consent to such bulk release for marketing and solicitation. Because the release is dependent on the person’s consent, section 2721(c) does not permit the resale of this information for any purpose except marketing and solicitation. *See* 18 U.S.C. § 2721(c) (“An authorized recipient under section (b)(12) may resell or redisclose personal information [only] pursuant to subsection (b)(12).”). Thus, according to the plain language of section 2721(c), a law enforcement agency cannot obtain personal information which was obtained in bulk based on the owner’s express consent under (b)(12), even though law enforcement agencies are authorized recipients under section 2721(b)(1). This is because Congress was being careful to limit resale to the exact purpose that the Missouri citizen had consented to. But under West’s interpretation, a

reseller need not qualify under any one of section 2721(b)'s exceptions and thus is not limited by any of these 2721(c) restrictions. It makes no sense to give such latitude to resellers and simultaneously restrict 2721(b)(12) recipients.

Given the strict linkage between the method of obtainment and the restrictions on resale, Congress could not have intended to create a gaping hole in the statute for resellers by authorizing them to obtain the entire driver's license database simply by identifying themselves as a reseller. At a minimum, if Congress sought to create a separate exception for resellers, it would have at least mentioned "resellers" and added a qualifying adjective such as "legitimate," as it did with respect to business use of personal information. 18 U.S.C. § 2721(b)(3) (personal information may be disclosed "[f]or use in the normal course of business by a *legitimate* business" (emphasis added)). In fact, given that wholesale resellers are businesses which sell information, Congress could easily have added a subsection (C) to 18 U.S.C. § 2721(b)(3) to permit such businesses to obtain DMV records for resale. It did not. Instead, all of the language of the statute, as well as the absence of any reference to wholesale resellers, shows that Congress did not intend for those resellers to have uniquely unfettered access to DMV records.

## **B. The Legislative History**

Even assuming that the text leaves any ambiguity regarding the limitations placed on "authorized recipients," the DPPA's legislative history also supports the Court's conclusion. According to the statement made by Congressman James P. Moran, the DPPA's sponsor in the House of Representatives:

Careful consideration was given to the common uses now made of this information and great efforts were made to ensure that those uses were allowed under this bill. Among those who will continue to have unfettered access are federal and state governments and their contractors, for use in auto recalls, by businesses (such as an insurance company) to verify the accuracy of personal information submitted by a licensee, for use in any civil or criminal proceeding, in research activities, and in marketing activities as long as the individual has been given the opportunity to opt out.<sup>2</sup>

*Protecting Driver Privacy: Hearings on H.R. 3365 Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 103d Cong., 2d Sess., 1994 WL 212698 (Feb. 3, 1994) [hereinafter *Statement of Rep. Moran*]. There is no mention here of the need for resellers to obtain drivers' personal information. Instead, the Congressman referred exclusively to the permissible uses listed in section 2721(b).

In the same statement, Congressman Moran focused primarily on "the need for individuals to have some control over how personal information about them is used." *Id.* He explained that the DPPA "prohibit[s]" the disclosure of personal information "about a licensee unless there is a *specific, approved reason for doing so.*" *Id.* (emphasis added).

Congressman Moran concluded his statement by asserting that "privacy is . . . a basic human right to which every person is entitled." *Id.* As this peroration suggests, while the DPPA strikes a balance with legitimate business and governmental concerns through the

---

<sup>2</sup> As *Taylor* explains, "[t]he 'opt out' provisions of the original legislation with respect to bulk distribution" under subsection (b)(12) "were changed to the 'opt in' provisions now in § 2721(b)(11) and (12) by the October 1999 amendments to the DPPA." 612 F.3d at 337 n.10 (citing Pub. L. No. 106-69, 113 Stat. 986 (Oct. 9, 1999)). This amendment was clearly intended to provide even greater protection for drivers' privacy.

exceptions enumerated in section 2721(b), the overriding purpose of the statute is plain by its title: The Driver's Privacy Protection Act. It would be inconsistent with this purpose to permit wholesale resellers to obtain all of the personal information that Congress sought to shield simply because they planned to resell it in the open market.

**C. Counterarguments in *Taylor* and *ChoicePoint***

Critics of the Court's interpretation have asked "why Congress would require resellers to actually use the records before reselling the records." *Taylor*, 612 F.3d at 338. But that question is of no relevance here. Congress did not require that the information had to be used before it was resold – nor did this Court intend to suggest that no information could be resold before it was used. *See Roberts*, 2008 WL 5234675 at \*3 (rejecting the "conten[tion] that section 2721(c) of the DPPA allows for re-sale or re-disclosure of personal information by a business entity, no matter the purpose for which that entity obtained the information"). Indeed, the Court's interpretation in *Roberts* never precluded a true agent from obtaining information for the purpose of facilitating its customer's permissible use and never held that an authorized recipient must use the information before reselling it.

The more relevant question is why Congress would limit resale to persons or entities that had obtained the information pursuant to one of the fourteen specific permissible uses. The answer is not surprising. Congress, like its constituents, feared that private information widely circulated in vast databases would be intentionally or inadvertently leaked, and there would be no practical way to identify the source of the



leak. Nor would there be a viable way to know whether unscrupulous individuals within recipient organizations were secretly trolling through drivers' personal information to learn about a neighbor or ex-girlfriend. Indeed, the DPPA's House sponsor recognized that the advent of computer technology made it increasingly difficult to control information: "Computers have enabled individuals with a click of a button to pull up a DMV record . . . [which] makes it more important that safeguards are in place to protect personal information." *Statement of Rep. Moran, supra*. By limiting the release of information to persons or entities with specific permissible purposes, the DPPA also limits the numbers of persons with access to personal information and maintains the balance between privacy and the societal needs expressed in the fourteen exceptions. This reasoning does not read the provision on resale out of existence, but it does prevent wholesale retailers' access to DMV databases containing every driver's private information, a result that is consistent with the language and structure of the legislation as well as its legislative history.

With respect to its interpretation of "authorized recipient," *Taylor* relied on *Russell v. ChoicePoint Services, Inc.*, 300 F. Supp. 2d 450 (E.D. La. 2004). *See Taylor*, 612 F.3d at 338 (noting *ChoicePoint*'s "careful analysis of 'authorized recipient'"). The *ChoicePoint* opinion concluded that "authorized recipient" in section 2721(c) of the DPPA refers to anyone authorized by a state DMV to purchase personal information from it. *Choice Point*, 300 F. Supp. 2d at 457. The judge reasoned that dictionaries commonly

define the term “authorize” as a grant of authority – e.g., by a state or municipal agency – and

[i]t is doubtful that Congress employed the term “authorized” to refer to the DPPA directly sanctioning a recipient because the Act otherwise speaks in terms of “use” rather than “user” and provides no process or guidelines for authorization. *More likely, Congress intended to leave the recipient authorization process to the states.*

*Id.* at 456 (emphasis added).

*ChoicePoint* also relies on legislative history to support its conclusion. By its logic, because Congress was aware that states sold driver’s license information to resellers and wanted to “strike ‘a critical balance between legitimate governmental and business needs for this information and the fundamental right of our people to privacy and safety’,” Congress must have intended to permit states to decide which recipients should obtain the information. *Id.* at 456 (citing 139 Cong. Rec. § 15, 763 (1993)). Hence, all those selected by the state to purchase personal information from it automatically become “authorized recipients” under section 2721(c) of the DPPA.

There are several problems with the analysis and conclusions in the *ChoicePoint* opinion. First, while stating that it relies on the plain language of the DPPA, *ChoicePoint* does not discuss the language of section 2721(c) that categorizes authorized recipients based on the subsection of 2721(b) “under” which the information is obtained. Section 2721(c)’s multiple references to section 2721(b) cannot be ignored. As previously explained, section 2721(c)’s careful treatment of (b)(11) and (b)(12) is inconsistent with the notion that Congress intended to give more latitude to wholesale resellers than to

entities obtaining information under an enumerated permissible use in section 2721(b). Moreover, *ChoicePoint*'s statement that the DPPA provides "no process or guidelines for authorization," *id.* at 456, is contrary to the express language in section 2721(b) listing fourteen exceptions to the general rule that drivers' personal information may not be sold.

It strains credulity even further to suggest that, in enacting federal legislation to limit the states' sales of their drivers' personal information, Congress delegated to the states the power to authorize any business to purchase from them and resell entire DMV databases (provided the resellers' customers check a box promising to comply with the DPPA). After all, the DPPA begins with the general prohibition: "A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity . . . personal information . . . except as provided in subsection (b) of this section." 18 U.S.C. § 2721(a). The Supreme Court's *Reno v. Condon* decision has become part of the Constitutional Law canon, teaching law students that the Tenth Amendment is no bar to federal regulation of states' sales of drivers' personal information. *Reno v. Condon*, 528 U.S. 141, 143 (2000) ("hold[ing] that in enacting this statute Congress did not run afoul of the federalism principles"). Yet *ChoicePoint* now suggests that Congress intended to delegate such regulation of the states to the states – the very sellers of drivers' personal information that Congress saw fit to restrict. *ChoicePoint*, 300 F. Supp. 2d at 456 ("Congress intended to leave the recipient authorization process to the states.").

Finally, the *ChoicePoint* opinion observes that in other consumer protection statutes Congress limited the distribution of information to specific persons (such as “a law enforcement agency” or “consumer” or “any person”) and Congress did not do so in the DPPA. Therefore, in the DPPA Congress must not have been concerned with who gets the information; Congress was only concerned with misuse of the information.

In fact, in the DPPA Congress did authorize specific types of persons to receive the information just as it did in the consumer statutes relied on by *ChoicePoint*. *See, e.g.*, 18 U.S.C. § 2721(b)(6) (insurance companies), (b)(1) (government agencies or law enforcement), (b)(3) (legitimate businesses), (b)(8) (private investigation agencies). But, because the DPPA is quite detailed and many types of entities or persons could qualify under some of the exceptions, it was not practical to list them all. *See, e.g.*, 18 U.S.C. §§ 2721(b)(7) (for use in providing notice to owners of towed vehicles); 2721(b)(4) (for use in connection with any civil or criminal proceeding). It does not follow from this linguistic structure that Congress intended that anyone could obtain every driver’s personal information so long as they did not misuse it. Otherwise, Congress could have written a shorter statute prohibiting only the *use* of personal information (except for the fourteen permissible uses), and there would have been no need to prohibit obtainment and disclosure as well. *See* 18 U.S.C. § 2724(a) (“A person who knowingly *obtains, discloses or uses* personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains.” (emphasis added)). Under such an alternative DPPA, when someone used a driver’s

personal information to stalk and kill them, the killer would face a penalty under the DPPA – no doubt an ineffective deterrent. In reality, rather than just attempting to deter stalkers by providing for their civil and criminal liability after the fact, Congress restricted the free flow of private information to prevent it from leaking out in the first place.

In summary, the Court interprets “authorized recipient” as any individual or entity, or their agent, that obtains personal information from DMV records for one of the permissible uses under section 2721(b). This reading of section 2721(c) is supported by dicta in *Reno v. Condon*. After listing section 2721(b)’s fourteen permissible purposes, Chief Justice Rehnquist equated authorized recipients under section 2721(c) with “private persons who have obtained drivers’ personal information for one of the aforementioned permissible purposes to further disclose that information for any one of those purposes.” *Reno v. Condon*, 528 U.S. at 146 (citing 18 U.S.C. § 2721(c)). This is also the most logical conclusion based on the language of the DPPA, the purpose of the statute, the legislative history, and common sense. The DPPA does not delegate to the states the decision of who is an “authorized recipient” as that term is used in the DPPA.

The *Taylor* court – apparently recognizing the problems with the reasoning in *ChoicePoint* – cites it approvingly without delving into the details of its analysis, adding only: “An authorized recipient would be under ‘subsection (b)(12),’ for example, *if* the state gives him the data for the purpose of reselling it to a person who uses it for marketing in conformity with (b)(12).” *Taylor*, 612 F.3d at 339 (emphasis added). *Taylor* seems to reason that because the state *could* disclose personal information

pursuant to one of the DPPA exceptions, Congress cross-referenced 2721(b) in every sentence of 2721(c) merely to suggest to the states that they might consider 2721(b) in deciding whether to designate under which 2721(b) exception the information was being given. The Court sees no other way to reconcile *Taylor*'s reliance on *ChoicePoint* with the ambiguous explanation quoted above. However, this opaque construction of section 2721(c) means that Congress was only making suggestions to the states about how to disclose the information, an interpretation that is at odds with normal congressional behavior and the purpose of the DPPA. Regardless, it is simply illogical that Congress intended to delegate to the states the right to decide who could purchase the DMV records, since the DPPA was passed specifically to restrict the states' sales of those DMV records.

For the reasons stated above, Defendant West's first argument fails. West is not an authorized recipient as a matter of law based on its mere purported "purpose of reselling information for permissible uses." [Doc. # 31 at 11.]

## **VII. Are Bulk Sales Generally Permissible under the DPPA?**

Even if Defendant West qualified as an authorized recipient, "[a]n authorized recipient of personal information . . . may resell or redisclose the information *only for a use permitted under subsection (b)*" of the DPPA. 18 U.S.C. § 2721(c) (emphasis added). Yet Defendant argues that "[a]bsent an allegation of misuse by West or its customers," the DPPA violation alleged in Plaintiff's Complaint is implausible because bulk sale of personal information is generally permissible under the statute. [Doc. # 40 at 9.] West

maintains: “That Congress did not intend to stop the practice of data aggregation and resale for permitted uses is confirmed by the fact that a number of the permissible uses expressly identified in the DPPA contemplate bulk obtainment.” [Doc. # 31 at 12 n.8, citing 18 U.S.C. § 2721(b) (2), (5); *Taylor*, 612 F.3d at 335-36.] An analysis of the text, structure, and legislative history of the DPPA again refutes West’s argument.

**A. Textual Analysis of Section 2721(b)**

Although acknowledging the ambiguity of section 2721(b), *Taylor* ultimately concludes that “Congress intended bulk distribution.” *Taylor*, 612 F.3d at 336; *see also* Laura S. Underkuffler, *Judicial Takings: A Medley of Misconceptions*, 61 *Syracuse L. Rev.* 203, 209-10 (2010) (“A state’s bulk sale of individuals’ driver’s license data to third parties, and the resale of that data to other parties, was upheld by an appellate court despite what appeared to be clear statutory law to the contrary.” (citing *Taylor*, 612 F.3d at 340)). According to *Taylor*, bulk sales of personal information are permitted by the DPPA as long as the recipient “does not actually use, or intend to use, any of the information in a manner prohibited by section 2721(b) . . . .” *Taylor*, 612 F.3d at 337. DMV records can always be sold in bulk even if the reseller’s customer has no existing permissible use under section 2721(b). Again, the Court must disagree.

*Taylor* correctly notes that only subsection (b)(11) explicitly refers to “individual motor vehicle records” and only (b)(12) explicitly refers to “bulk distribution”; for “the remaining twelve permissible uses, the statute seems to have more than one reasonable interpretation: individual release, bulk release, or both.” *Id.* at 335. *Taylor* reasons that it

would “not make sense that Congress would expressly limit states to individual distribution with one permissible use if Congress intended to limit *all* of the permissible uses to individual distribution,” and therefore concludes that Congress intended bulk distribution. *Id.* at 336.

In reaching this conclusion, *Taylor* first misapplied the maxim of *expressio unius est exclusio alterius*. *Taylor* applied its version of the rule: “Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.” *Id.* (quoting *Arif v. Mukasey*, 509 F.3d 677, 681 (5th Cir. 2007)). However, the *expressio unius* maxim – “the expression of one thing is the exclusion of another” –

does not apply to every statutory listing or grouping. It has force only when the items expressed are members of an associated group or series, justifying the inference that the items not mentioned were excluded by deliberate choice. . . . [For example, a] statute which provides that a thing shall be done in a certain way carries with it an implied prohibition against doing that thing in any other way.

2A *Sutherland Statutory Construction*, *supra*, § 47:23, at 405-413. Moreover, “there should be some evidence the legislature intended its (*expressio unius*) application lest it prevail as a rule of construction despite the reason for and the spirit of the enactment.” *Id.* § 47:25, at 437 (internal quotation omitted).

The fact that only subsection (b)(11) explicitly refers to “individual motor vehicle records,” only (b)(12) explicitly refers to “bulk distribution,” and the twelve remaining



subsections are silent on the manner of distribution does not justify *Taylor*'s inference that Congress could not have intended to generally limit the permissible uses to individual distribution. One could more plausibly infer that Congress would not expressly permit states to distribute personal information in bulk for just one permissible use if Congress intended to permit bulk distribution for all of the permissible uses. Such an interpretation is far more consistent with the DPPA's primary purpose – to protect drivers' privacy.

Indeed, “[t]he enumeration of exclusions from the operation of a statute indicates that the statute should apply to all cases not specifically excluded.” *Id.* § 47:23, at 418. As previously explained, the specific uses permitted under section 2721(b) are enumerated exceptions to a general rule banning the sale of drivers' personal information. *See* 18 U.S.C. § 2721(a) (“In general” prohibiting disclosure of personal information “except as provided in subsection (b)”). That general rule of nondisclosure must be applied to all uses not specifically excluded by section 2721(b), and bulk distribution is only specifically excluded in subsection (b)(12).

Even assuming that Congress did not intend to limit all of the permissible uses to individual distribution, it does not follow that bulk distribution is always permissible under the statute so long as the recipient “does not actually use, or intend to use, any of the information in a manner prohibited by section 2721(b) . . . .” *Taylor*, 612 F.3d at 337. Again, there is no listing of “prohibited” uses under section 2721(b), which is entitled “Permissible uses” and lists only exceptions to the general rule against disclosure. 18 U.S.C. § 2721(b). In fact, nowhere does the DPPA enumerate any “prohibited purposes”

or “prohibited uses.” Rather, the statute generally prohibits all but the fourteen permissible uses enumerated in section 2721(b). The title of the entire section 2721 is “Prohibition on release and use of certain personal information from State motor vehicle records” – again illustrating that prohibition is the general rule, not the exception as *Taylor* would have it. 18 U.S.C. § 2721.

The DPPA is not a model of statutory drafting, but if it means anything at all it is this: A potential stalker cannot walk into a Missouri DMV to obtain every Missouri driver’s name, address, height, weight, eye color, driver’s license number, and social security number without a specific permissible use under the DPPA. *See Taylor*, 612 F.3d at 336 (explaining that the immediate impetus for the DPPA was “the murder of actress Rebecca Schaeffer at the hands of a stalker”). It is not enough for him to smile, nod, and promise to comply with the DPPA in the future. Rather, he must at least be able to articulate a specific permissible use from among the closed universe of permissible uses under section 2721(b), beyond which all uses are impermissible. If the same standard is not applied to resellers, then the DPPA does not prevent them from selling everyone’s personal information on websites such as [www.publicdata.com](http://www.publicdata.com), so long as the purchaser promises not to misuse it.

The DPPA creates a private right of action for “the individual” whose personal information was knowingly obtained, disclosed, or used “for a purpose not permitted” under section 2721(b). 18 U.S.C. § 2724(a). “It shall be unlawful for any person knowingly to obtain or disclose personal information . . . for *any* use not permitted under

section 2721(b) of this title.” 18 U.S.C. § 2722(a) (emphasis added). And an “authorized recipient . . . may resell or redisclose the information only for a use permitted under subsection (b) . . . .” 18 U.S.C. § 2721(c). Therefore, the sale of any individual’s personal information – the quantum of data used throughout the statute – violates the DPPA whenever it is not matched with an identifiable permitted use that is relevant to “the individual to whom the information pertains.” 18 U.S.C. § 2724(a).

## **B. The Structure of Section 2721(b)**

To interpret the DPPA, it is necessary to view each permissible use under section 2721(b) in the context of all fourteen of those exceptions to the general rule prohibiting the obtainment, use, and disclosure of drivers’ personal information. As previously discussed, those fourteen exceptions are:

(1) *For use* by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.

(2) *For use* in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.

(3) *For use* in the normal course of business by a legitimate business or its agents, employees, or contractors, *but only*-

(A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and

(B) if such information as so submitted is not correct or is no longer

- correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.
- (4) *For use* in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.
- (5) *For use* in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.
- (6) *For use* by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.
- (7) *For use* in providing notice to the owners of towed or impounded vehicles.
- (8) *For use* by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection.
- (9) *For use* by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49.
- (10) *For use* in connection with the operation of private toll transportation facilities.
- (11) *For any other use* in response to requests for individual motor vehicle records if the State has obtained the *express consent* of the person to whom such personal information pertains.
- (12) *For bulk distribution* for surveys, marketing or solicitations if the State has obtained the *express consent* of the person to whom such personal information pertains.
- (13) *For use by any requester*, if the requester demonstrates it has obtained the *written consent* of the individual to whom the information pertains.

(14) *For any other use* specifically authorized under the law of the State that holds the record, if such use is *related to the operation of a motor vehicle or public safety*.

18 U.S.C. § 2721(b) (emphasis added).

The structure of section 2721(b) is relatively straightforward. Subsections (b)(1) through (10) identify specific uses of personal information that are permissible under the DPPA – e.g., “to verify the accuracy of personal information submitted by the individual to the business . . . and . . . if such information as so submitted is not correct or is no longer correct, to obtain the correct information . . . .” 18 U.S.C. § 2721(b)(3). Subsections (b)(11) through (14), however, provide for potentially less-restrictive exceptions, therefore adding heightened requirements. Subsection (b)(11) directly follows the ten specific uses of individuals’ DMV records, providing a catch-all exception “[f]or any other use in response to requests for individual motor vehicle records,” but only with the individual’s express consent. 18 U.S.C. § 2721(b)(11). Subsection (b)(13) allows any “requester” to walk into a DMV to obtain an individual’s personal information, but only with the individual’s written consent. 18 U.S.C. § 2721(b)(13). Subsection (b)(14) provides a catch-all exception “[f]or any other use specifically authorized under the law of the State” and relating to motor vehicles or public safety. 18 U.S.C. § 2721(b)(14). The other potentially less-restrictive exception, subsection (b)(12), allows bulk distribution for commercial purposes, but only with the individual’s express consent – indicative of the atypicality of commercial bulk distribution among the permissible purposes. 18 U.S.C. § 2721(b)(12).

In fact, as previously discussed, two of these more open-ended exceptions with heightened requirements, subsections (b)(11) and (12), are singled out for special treatment in section 2721(c). Most tellingly, “[a]n authorized recipient under (b)(12)” – i.e., a recipient of the information of individuals who have expressly consented to bulk distribution for surveys, marketing, or solicitations – “may resell or redisclose personal information pursuant [only] to subsection (b)(12).” 18 U.S.C. § 2721(c); *see* 2A *Sutherland Statutory Construction, supra*, § 47:23, at 398-404 (“As the [*expressio unius*] maxim is applied to statutory interpretation, where a form of conduct, the manner of its performance and operation, and persons and things to which it refers are designated, there is an inference that all omissions should be understood as exclusions.”). Unlike every other permitted use of personal information, the information pertaining to an individual who has expressly consented to bulk distribution may not be diverted for any other permissible use, even those uses that would never have required the individual’s express consent. The only reason for such a provision is that Congress intended to limit commercial bulk distribution, absent consent. The Supreme Court has expressed a “preference for avoiding surplusage constructions,” *Lamie v. United States Trustee*, 540 U.S. 526, 536 (2004), yet *Taylor*’s interpretation of the DPPA would render mere surplusage section 2721(c)’s cautious treatment of bulk distribution under (b)(12).

It should be noted that subsection (b)(5) may also envision bulk distribution, but only for research purposes, and only “so long as the personal information is not published, redisclosed, or used to contact individuals.” 18 U.S.C. § 2721(b)(5). Certain

government functions or motor-vehicle-related activities could also conceivably entail bulk transfers. *See* 18 U.S.C. § 2721(b). However, in such cases, by definition, all drivers would fit within the identifiable permissible use at the moment of obtainment and disclosure. Commercial bulk distribution would still be prohibited when based on the mere possibility that an individual could fit within some permissible use at some point in the future.

### **C. The Legislative History**

To the extent that the DPPA text is ambiguous with respect to the bulk sales issue, and in case the statute's title is not clear enough, the legislative history reveals the overriding purpose of the DPPA: to protect drivers' privacy. Given such a purpose, the interpretation most consistent with Congressional intent requires that disclosure of personal information be narrowly tailored to a specific permissible purpose.

It is true, as *Taylor* notes, that Congressman Moran stated:

Among those who will continue to have unfettered access are federal and state governments and their contractors, for use in auto recalls, by businesses (such as an insurance company) to verify the accuracy of personal information submitted by a licensee, for use in any civil or criminal proceeding, in research activities, and in marketing activities as long as the individual has been given the opportunity to opt out. *The bill would allow DMVs to continue to sell DMV information in bulk as long as every driver in that state had been given the opportunity to restrict the sale of their name for marketing purposes.*

*Statement of Rep. Moran, supra* (emphasis added). Congressman Moran simply referred, in order, to subsections (b)(1) (government agencies), (b)(2) (auto recalls), (b)(3) (legitimate businesses to verify the accuracy of information submitted to it), (b)(4) (civil

or criminal proceedings), (b)(5) (research activities), and (b)(12) (bulk distribution for marketing activities). *See* 18 U.S.C. § 2721(b).

In the same statement, Congressman Moran explained that the DPPA was “designed to give individuals control over the release of their personal information and give them the opportunity to make choices as to whether this information is released, not just for individual look-ups, but also for release in bulk.” *Statement of Rep. Moran, supra*. He even went so far as to spell out the core values behind the DPPA:

The basic concept behind this legislation is the philosophy first coined by Congressman Ed Markey: knowledge, notice, and no. Knowledge: individuals should have knowledge of how personal information about them will be used. Notice: they should have notice when personal information about them is sold/resold. No: they should have the right to object to those uses/reuses.

*Id.*

*Taylor*’s interpretation of the DPPA turns the requirement of a “specific, approved reason” on its head, depriving individuals of “knowledge, notice, and no.” *Id.* First, individuals would have little knowledge of how their personal information is used, as it moves in bulk from the DMV toward internet clearinghouses such as [www.publicdata.com](http://www.publicdata.com). Second, individuals would have no “notice when personal information about them is sold/resold.” *Id.* And third, it is important to note that individuals originally had to object to bulk sale of their personal information for commercial purposes under section 2721(b)(12). “The ‘opt out’ provisions of the original legislation with respect to bulk distribution” was “changed to the ‘opt in’ provisions now



in § 2721(b)(11) and (12) by the October 1999 amendments to the DPPA.” *Taylor*, 612 F.3d at 337 n.10 (citing Pub. L. No. 106-69, 113 Stat. 986 (Oct. 9, 1999)). In other words, the DPPA originally put the burden on individuals to avail themselves of “[t]he ‘opt out’ provisions . . . with respect to bulk distribution,” but Congress later shifted that burden to provide even greater privacy to drivers. *Id.* Drivers must now “opt in” to (b)(12), which is the only reference to bulk distribution in the DPPA and is treated with great care by section 2721(c). Since Congress intended to allow individuals to object to bulk distribution of their personal information by opting out (and it subsequently strengthened privacy protection by allowing for commercial bulk distribution only when individuals opt in), it is illogical to now claim that Congress always intended bulk distribution for all exceptions listed in 2721(b).

It is hard to imagine an interpretation of the DPPA less in keeping with Congressional intent than one which allows bulk sales of personal information as the default rule. In practice, *Taylor*’s interpretation means that the vast majority of the personal information sold is not put to an authorized use. It strikes no balance at all to allow resellers to disseminate in mass millions of drivers’ personal information. Instead, by focusing on “specific, approved reasons,” Congress accommodated particular commercial needs while preventing wholesale distribution of personal information for which there is only a hypothetical use. *Statement of Rep. Moran, supra*.

Furthermore, while Congressman Moran in 1994 referred to the DPPA’s exceptions for legitimate “common uses now made of this information,” *id.*, *Taylor* condones novel

uses of personal information that could be facilitated by bulk distribution without the individual's consent. While Congressman Moran warned that advances in computer technology "make[ ] it more important that safeguards are in place to protect personal information," *id.*, *Taylor* argues:

At a checkout line at a grocery store or similar establishment, when a customer wishes to pay by (or cash) a check, and presents a driver's license as identification, it is obviously wholly impractical to require the merchant for each such customer to submit a separate individual request to the state motor vehicle department to verify the accuracy of the personal information submitted by the customer, under section 2721(b)(3).

612 F.3d at 337. Thus, *Taylor* assumes that a business has the right to possess an individual's personal information even if that individual never walks into its store; it also apparently assumes that any employee working a cash register could access the personal information of every driver in the state. In reality, when an individual pays by check or credit card at the grocery store, the cashier rarely asks for identification. When they do, the employee merely confirms that the names on the cards match and that the individual resembles the photograph on the driver's license. For other transactions – e.g., purchasing an automobile or applying for a credit card – a business would have time to avail itself of subsection 2721(b)(3) to verify the identity of an individual.

Such a process of matching individuals to specific permissible uses should not "flood the state department with more requests than it could possibly handle." *Id.* at 337.

This empirical claim – offered as evidence of Congressional intent – simply has not been proven. Discovery may shed some light on various states’ policies with respect to the manner of disclosure of personal information.

*Taylor* also warned: “Ninety thousand [credit card] applications are processed daily. That alone may be 90,000 requests that a state would have to individually verify every day.” *Taylor*, 612 F.3d at 338 n.12. Aside from its failure to divide by fifty, *Taylor*’s suggestion that the states must be at the beck and call of credit card companies is misleading. It may be the case that technology exists which would allow authorized recipients to download specific individuals’ personal information from a secure site to sell to customers having a specific permissible use. Even if the cost of protecting drivers’ privacy is that a credit card company is momentarily delayed before issuing some of the thousands of cards approved daily, such a balance is consistent with Congressional intent. Furthermore, there are many other ways to gather consumer data. Understandably, it is more convenient to obtain every driver’s personal information in one reliable place. But Congress recognized that consumers have an interest in maintaining the privacy of their *coerced* personal information until there is a reason to release it.

The final specter raised by *Taylor* is “vast potential liquidated damages.” *Taylor*, 612 F.3d at 330. According to section 2724(b):

The court may award –

- (1) actual damages, but not less than liquidated damages in the amount of \$2,500;

(2) punitive damages upon proof of willful or reckless disregard of the law;

(3) reasonable attorneys' fees and other litigation costs reasonably incurred; and

(4) such other preliminary and equitable relief as the court determines to be appropriate.

18 U.S.C. § 2724(b). As the Eleventh Circuit has explained:

Section 2724(b) begins, “[t]he Court *may* award.” The use of the word “may” suggests that the award of any damages is permissive and discretionary. . . . [W]e conclude that the use of the word “may” implies a degree of discretion. Thus, the district court, in its discretion, may fashion what it deems to be an appropriate award.

*Kehoe v. Fid. Fed. Bank & Trust*, 421 F.3d 1209, 1217-18 (11th Cir. 2005) (citations omitted). As the Eleventh Circuit suggests, the DPPA grants the Court discretion in fashioning an appropriate remedy sufficient to deter future violations. There is no reason to expect that if courts enforce the DPPA as written that they will make large (or any) damage awards. The goal is compliance with the law, not windfall rewards. Further, just because damages are authorized by a statute does not mean the language of the statute and the intent of Congress can be ignored. If Congress makes a mistake, it is the responsibility of Congress to fix it. It is not the role of the courts to rewrite the legislation.

For the reasons stated above, Defendant's second argument – that absent an allegation of misuse by West or its customers, the DPPA violation alleged in Plaintiff's Complaint is implausible because bulk sale of personal information is generally

permissible – also fails. Accepting as true all facts plead by Plaintiff Johnson, the Court cannot say that West is entitled to judgment as a matter of law.

### **VIII. Standing**

Defendant West also argues that Plaintiff Johnson and the putative class members do not have standing to sue because they have suffered no injury-in-fact. Article III standing requires a plaintiff to have suffered an injury-in-fact that has a causal connection with the complained-of conduct that is likely to be redressed by a favorable decision. *Pucket v. Hot Springs Sch. Dist.*, 526 F.3d 1151, 1157 (8th Cir. 2008) (citing *Steger v. Franco, Inc.*, 228 F.3d 889, 892 (8th Cir. 2000)); *see also Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992). “At the pleading stage, general factual allegations of injury resulting from the defendant’s conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim.” *Lujan*, 504 U.S. at 561; *see also H.L. v. Matheson*, 450 U.S. 398, 414 (1981) (“Standing depends initially on what the complaint alleges . . . as courts have the power only to redress or otherwise to protect against injury to the complaining party” (citations omitted)).

The Complaint alleges that “[t]he personal information or highly restricted personal information of *Plaintiff and the putative Class members* was obtained and disseminated by Defendant for purposes not permitted under the DPPA.” [Doc. # 1 at ¶ 13 (emphasis added).] Plaintiff has clearly alleged that she and fellow class members suffered an injury-in-fact caused by Defendant’s violations of the DPPA.

The DPPA is designed to protect personal information. *Parus v. Cator*, No. 05-C-0063-C, 2005 WL 2240955 (W.D. Wis. Sept. 14, 2005) (citing 139 Cong. Rec. S15765 (1993)). It protects drivers' privacy by placing restrictions on the purposes for which personal information may be obtained, used, and disclosed. In fashioning the DPPA, Congress created a right to privacy, the invasion of which creates an injury sufficient to create standing. *See generally Pichler v. UNITE*, 542 F.3d 380, 388 (3d Cir. 2008) (recognizing that the DPPA protects the privacy rights of individuals); *Parus*, 2005 WL 2240955 at \*5 (finding that improperly obtaining personal information was an injury for purposes of a DPPA claim). In alleging a violation of that right, Plaintiff has adequately alleged a basis for standing.

#### **IX. Conclusion**

Accordingly, it is hereby ORDERED that Defendant West's Motion for Judgment on the Pleadings [Doc. # 30] is DENIED.

s/ Nanette K. Laughrey  
NANETTE K. LAUGHREY  
United States District Judge

Dated: August 3, 2011  
Jefferson City, Missouri